Coding for Optical Channels With Photon-Counting

R. J. McEliece and L. R. Welch
Communications Systems Research Section

We study the problem of coding for Pierce's recent model for optical communication. We conclude that for any positive rate ρ (measured in nats per photon), the best code of length n has an error probability bounded by an exponentially decaying function of n; we exhibit explicit practical schemes for $\rho \leqslant \sim 1$; and give evidence that $\rho \approx 1$ may be the "practical limit" for optical communication.

I. Introduction

In a recent paper Pierce (Ref. 1) has shown that if one uses photon-counting techniques for communication at optical frequencies, and low noise temperatures, the rate at which one can operate is at most $hf/kt = 4.80 \times 10^{-11}$ (f/T) nats per photon, where f is the photon frequency in hertz and T is the noise temperature in kelvin. This number is typically fairly large; for example $f = 6 \times 10^{14}$ Hz, $T = 400$ K gives a limit of 72 nats per photon. Pierce observed, however, that if one attempts to design a practical communication system for such a channel, one encounters severe problems of coding complexity long before the limiting rate of hf/kT is reached. Moreover, these problems are not caused by thermal noise, but rather by the nature of the photon-counting process itself. We shall now describe Pierce's "noiseless" photon channel, and devote the rest of our article to a discussion of the coding problem for this channel.

We assume that the data to be transmitted consists of a long stream of 0's and 1's: $x_1, x_2, x_3, \ldots$, and that the time interval during which these bits are to be transmitted is divided into small intervals ("slots") of duration t_0 seconds each. The transmitter is a semiconductor laser which is pulsed during the ith time interval if and only if $x_i = 1$. The expected number of photons emitted during such a pulse we denote by λ. The receiver is a photon counter; it emits a 1 if it is struck by one or more photons in a given time slot, and a 0 if it is not. If the laser is not pulsed, of course it emits no photons; hence a transmitted 0 is always received correctly. On the other hand, if the laser is pulsed, because of the Poisson statistics which govern photon emissions, there is a nonzero probability $e^{-\lambda}$ that no photons will be emitted. Hence a transmitted 1 is received incorrectly as a 0 with probability $e^{-\lambda}$. In effect, then, the photon channel is just the "Z-channel" familiar to information theorists (see Fig. 1), where the crossover probability ϵ is equal to $e^{-\lambda}$.

In Ref. 1 Pierce considered the following coding scheme for this channel. There are n distinct binary codewords, each of length n. Each codeword has a 1 in one coordinate only. Since there are n codewords, each carries $\log n$ nats[1] of information. Furthermore, the transmission of each codeword requires exactly one pulse and hence an average of λ photons. Hence the rate of transmission, measured in nats per photon, is given by $\rho = (\log n)/\lambda$. The probability that the codeword will be received incorrectly is just the probability $e^{-\lambda}$ that no photons will be emitted by the laser during one pulse period. Since $\lambda = \rho^{-1} \log n$, it follows that if we use this

[1] Throughout the paper all logarithms will be natural.

scheme at a rate of ρ nats per photon, the error probability will be

$$P_E = n^{-(1/\rho)} \tag{1}$$

Hence for any desired rate of transmission ρ, however large, by choosing n large enough, one can make the receiver error probability arbitrarily small.

In practice, however, Pierce's codes are not of much use, unless ρ is quite small. For example, at $\rho = 1$ nat per photon, and $P_E = 10^{-6}$, Eq. (1) implies that n must be at least 10^6. The problem is of course that the decay of P_E in n and ρ is very slow. In Ref. 2 it was shown that there exist codes of length n for which P_E decays exponentially as a function of ρ^{-1}, $\rho \to 0$. In this paper we shall show that for any fixed value of ρ, however large, there exists a sequence of codes of increasing length all having rate at least ρ nats per photon, whose error probabilities decay exponentially as a function of the code length. In Section II we will prove this fact (the main idea of the proof is to use Pierce's coding scheme as a modulation scheme for more complex codes); in Section III we will exhibit some codes which are practical and give good performance for $\rho \leqslant \sim 1$ nat per photon. (These simple codes will outperform any possible coding strategy if one uses coherent signal amplification rather than photon-counting techniques, because $\rho = 1$ nat/photon is the *capacity* of the optical channel when linear amplification is used (Ref. 1). Finally, in Section IV we will give evidence (but no proof) that it is probably very difficult to design practical systems that operate at rates much larger than 1 nat per photon.

II. An Exponential Error Probability Bound

In this section we will show that there exists a function $E(\rho)$, which is positive for all $\rho > 0$, such that for any $\rho > 0$ there exists a sequence of codes $C_1, C_2, C_3, \ldots$, of increasing block length, each having rate at least ρ nats per photon, such that the decoding error probability for the kth code satisfies

$$P_E \leqslant \exp\left[-n_k E(\rho)\right], \tag{2}$$

where n_k is the length of the kth code.

Thus let $\rho > 0$ be fixed. Choose a positive integer q satisfying

$$q > e^{\rho}. \tag{3}$$

Having selected q, choose a real number R, $0 < R < 1$, satisfying

$$-\frac{1}{R}\log(1 - R) < \rho^{-1}\log q. \tag{4}$$

(This is possible since by Eq. (3) $\rho^{-1} \log q > 1$; and the left side of Eq. (4) is an increasing function of R and approaches 1 as $R \to 0$).

Now consider a q-ary erasure channel with erasure probability ϵ. This channel has input alphabet $A_q = \{1,2, \ldots, q\}$ and output alphabet $A'_q = A_q \cup \{e\}$, where "e" is an erasure symbol. The channel's transition probabilities are

$$P(y \mid x) = \begin{cases} 1 - \epsilon & \text{if } \; x = y \\ \epsilon & \text{if } \; y = e \\ 0 & \text{otherwise} \end{cases}$$

Thus each symbol is transmitted correctly with probability $1 - \epsilon$, and "erased" with probability ϵ. This channel has capacity $(1 - \epsilon)\log q$, and so according to the noisy-channel coding theorem (see Ref. 3, Chapter 5), for any $R < (1 - \epsilon)$, and any positive integer N there exists a code of length N with at least q^{RN} codewords, whose decoding error probability satisfies

$$P_E \leqslant \exp\left[-NE_r(R)\right], \tag{5}$$

where $E_r(R)$, the random coding exponent for the channel, is a function which is positive for all $R < 1 - \epsilon$.

Our object is now to use these codes, on the "photon Z-channel." To do this we must have a "modulation" scheme which will allow us to transmit symbols from $A_q = \{1,2, \ldots, q\}$ over the Z-channel. The modulation scheme we use is as follows: we assign each symbol from A_q a unique binary vector of length q containing one "1." For example, with $q = 4$ the assignment could be

1 : 1000
2 : 0100
3 : 0010
4 : 0001

(This is exactly Pierce's quantized pulse position modulation described in Ref. 1 and Section 1.)

When one of these length q binary patterns is transmitted over the Z-channel, the "demodulator" looks for a "1" among the q received bits; if a "1" is detected in the kth position, the demodulator knows for certain that the transmitted symbol was k. If, however, no 1's are detected, the demodulator has no idea what was sent and outputs the erasure symbol "e." It follows that when this particular modulation scheme is adopted, the Z-channel becomes a q-ary erasure channel whose erasure probability ϵ is equal to the crossover probability of the Z-channel.

The code of length N has at least q^{RN} codewords and so each codeword conveys at least $RN \log q$ nats of information. Since transmission of each codeword requires exactly N pulses, we are getting at least $R \log q$ nats per pulse. If we are transmitting at rate ρ nats per photon, this means that we need at most,

$$\lambda = \rho^{-1} R \log q \text{ photons per pulse.} \tag{6}$$

Hence if we operate the laser at λ photons per pulse, where λ is given by Eq. (6), our coding scheme will operate at ρ nats per photon. Now according to the Poisson statistics governing photon emission, this means that the erasure probability ϵ for the q-ary erasure channel is

$$\epsilon = q^{-R/\rho} \tag{7}$$

Hence if the code's (q-ary) rate R is less that the channel's (q-ary) capacity $1 - \epsilon$, we can get exponential decay of the error probability. This condition is

$$R < 1 - q^{-R/\rho}, \tag{8}$$

which is just a restatement of Eq. (4). Hence it follows that for every N there exists a code of rate R, whose error probability satisfies Eq. (5). This code, viewed as a code for the Z-channel, has length $n = qN$, and so its error probability satisfies

$$P_E \leqslant \exp[-nE_r(R)/q]. \tag{9}$$

Since for fixed $\rho > 0$, and q,R satisfying Eqs. (3) and (4) we have $E_r(R)/q > 0$, it follows that there exists a function $E(\rho)$ such that

$$P_E \leqslant \exp[-nE(\rho)], \tag{10}$$

which is what we set out to prove.

We have made no attempt to give numerical bounds on $E(\rho)$; it would be interesting to do this, however.

In the next section, we will show how the technique just described can be used to design practical coding schemes for the photon channel in the range $\rho \leqslant \sim 1$ nats/photon.

III. Practical Schemes for $\rho \leq \sim 1$

In this section we will give explicit examples of the coding schemes described in Section II; these will turn out to be easily implemented and have low error probabilities, provided ρ is not much larger than 1 nat/photon.

As before, for a given rate ρ, choose a positive integer $q > \exp(\rho)$. Using the modulation scheme described in Section II, the Z-channel becomes a q-ary erasure channel, and we must design a code over the alphabet A_q capable of correcting as many erasures as possible. An obvious choice is the class of Reed-Solomon codes, which require only that q be a power of a prime.

Over the alphabet A_q (which we now view as a finite field), Reed-Solomon codes are linear cyclic codes of length $n = q - 1$, arbitrary dimension $1 \leqslant k \leqslant n - 1$, with minimum distance $d = n - k + 1$. They will correct any pattern of up to $n - k$ erasures, and very efficient encoding and decoding procedures are known, when q is a power of 2 (see Ref. 5, Chapter 8 for details).

If we use an (n,k) Reed-Solomon code for the present application, each of the q^k codewords carries $k \log q$ nats of information, and each codeword requires n pulses. Thus if we are transmitting at ρ nats/photon, the average number of photons per pulse is at most (cf. Eq. (6)).

$$\lambda = \frac{k}{n} \cdot \rho^{-1} \log q \text{ photons per pulse.} \tag{11}$$

It follows that the erasure probability for the corresponding q-ary erasure channel is (at worst)

$$\epsilon = e^{-\lambda} = q^{-R/\rho}, \tag{11a}$$

where $R = k/n$ is the code rate. Since the RS code can correct all patterns of up to $n - k$ erasures, it follows that the decoding error probability P_E satisfies

$$P_E \leqslant \sum_{j=n-k+1}^{n} \binom{n}{j} \epsilon^j (1 - \epsilon)^{n-j}. \tag{12}$$

In Fig. 2 we have plotted P_E vs ρ for four typical RS codes. The curve labelled $q = 16$ is a (15,8) RS code with $q = 16$; the others are (31,16) $q = 32$; (63,32), $q = 64$; and (127,64), $q = 128$. It is seen that the performance of all of these codes degrades rapidly as ρ increases beyond 1. (It is to be recalled that as codes for the photon channel, the length is actually $16 \cdot 15 = 240$ for the $q = 16$ codes; $n = 31 \cdot 32 =$

992 for the q = 32 code; n = 4032 for q = 64; and n = 16256 for q = 128.) Each of these codes is the best of its length, at least in the limit as $\rho \to 0$, and so no significant improvement could be expected merely by altering the code's rate. We conclude that for $\rho \leqslant \sim 1$ practical schemes exist. In the next section we give evidence that $\rho \geqslant \sim 1$ may be very hard to achieve.

IV. R_0 for the Photon-Detection Channel

Associated with any discrete memoryless channel there is a number C, called channel capacity, which represents the theoretical maximum rate at which one can communicate reliably over the channel. However, it is usually extremely difficult to operate at rates very close to C, and it has been conjectured (see e.g., Ref. 4) that another number, R_0, which is associated with every discrete memoryless channel, is a more realistic measure of the maximum rate of practical reliable communication. In this section we shall show that for our photon-counting Z-channel, the value of ρ corresponding to R_0 is exactly 1 nat/photon; this number, incidentally, is the limiting value (capacity) for coherent optical communication systems (Ref. 1).

Given a discrete memoryless channel with input alphabet A_X, output alphabet A_Y, and transition probabilities $p(y|x)$, we can state the "R_0-conjecture" as follows. "Any practical communication system, in which the relative frequencies with which the input symbols $x \in A_X$ are used are described by the probability distribution $p(x)$, must operate at a rate R satisfying

$$R < \sim -\log \sum_{y \epsilon A_Y} \left[\sum_{X \epsilon A_X} p(x) \sqrt{p(y|x)} \right]^2 = R_0(p).\text{"} \qquad (13)$$

In the specific case of the Z-channel with erasure probability ϵ, with $p(x{=}0) = 1 - \delta$, $p(x{=}1) = \delta$, the quantity on the right side of Eq. (13) is given by

$$R_0(\delta) = -\log\left[1 - 2\delta(1-\delta)(1-\epsilon^{1/2})\right]. \qquad (14)$$

If we are using a code of length n and rate R for the photon-counting Z-channel, in which the average number of 1's per codeword is δn, a calculation similar to that which led to Eq. (16) and Eq. (11) shows that the average number of photons per pulse must be

$$\delta = R/\rho\delta \text{ photons per pulse.} \qquad (15)$$

Thus the erasure probability for the Z-channel is

$$\epsilon = \exp(-R/\rho\delta) \qquad (16)$$

and the inequality Eq. (13) becomes

$$R < -\log\left\{1 - 2\delta(1-\delta)\left[1 - \exp(-R/2\rho\delta)\right]\right\} \qquad (17)$$

Our result is the following.

Theorem: There exist real numbers (R,δ) $0 < R < \log 2$, $0 < \delta < 1$ satisfying Eq. (17) if and only if $\rho < 1$. Hence any system for the photon-counting Z-channel for which $\rho \geqslant 1$ must violate Eq. (13).

Proof: First assume $\rho < 1$, and define $\alpha = R/2\delta$. Then $\alpha > 0$ and Eq. (17) becomes

$$2\alpha\delta < -\log\left\{1 - 2\delta(1-\delta)\left[1 - \exp(-\alpha/\rho)\right]\right\}. \qquad (18)$$

Now choose α satisfying

$$\alpha < 1 - e^{-\alpha/\rho} \qquad (19)$$

(This is possible since $\rho \leqslant 1$.) For this fixed value of α the right side of Eq. (18) is equal to $2\delta(1 - e^{-\alpha/\rho}) + 0(\delta^2)$. It follows that Eq. (18) is satisfied for all sufficiently small $\delta > 0$. Thus with $R = 2\alpha\delta$ and δ small enough, Eq. (17) is satisfied.

Now assume $\rho \geqslant 1$. Then $\exp(-\alpha/\rho) \geqslant \exp(-\alpha)$, and the right side of Eq. (18) is bounded as follows:

$$-\log\left\{1 - 2\delta(1-\delta)\left[1 - \exp(-\alpha/\rho)\right]\right\}$$

$$\leqslant -\log\left\{1 - 2\delta(1-\delta)\left[1 - \exp(-\alpha)\right]\right\} \qquad (20)$$

If we replace the right side of Eq. (18) by its upper bound (Eq. 20)), a little rearrangement yields

$$\frac{1 - \exp(-2\alpha\delta)}{1 - \exp(-\alpha)} < 2\delta(1 - \delta). \qquad (21)$$

Lemma: Let $k > 0, f(y) = (1 - y^k)/(1 - y)$. Then

$$\inf_{0<y<1} f(y) = \begin{cases} k & \text{for } k < 1 \\ 1 & \text{for } k \geqslant 1. \end{cases}$$

(The proof of the lemma is elementary and is omitted.)

Now let $y = \exp(-\alpha)$, $k = 2\delta$. Then the left side of Eq. (21) is $(1 - y^k)/(1 - y)$. By the lemma, this is $\geqslant 2\delta$ if $2\delta < 1$; thus Eq. (21) implies $2\delta < 2\delta(1 - 2\delta)$, a contradiction. If $2\delta \geqslant 1$, then Eq. (21) gives $1 \leqslant 2\delta(1 - \delta)$, another contradiction, since $2\delta(1 - \delta) \leqslant 1/2$ for $0 < \delta < 1$. This completes the proof of the theorem.

References

1. Pierce, J. R., "Optical Channels: Practical Limits with Photon Counting," *IEEE Trans. Comm.,* COM-26 (1978), pp. 1819-1821.

2. Baumert, L. D., McEliece, R. J., and Rumsey, H. C., Jr., "Coding for Optical Channels," *DSN Progress Report 42-49,* Jet Propulsion Laboratory, Pasadena, Calif., Feb. 15, 1979, pp. 70-77.

3. Gallager, R. G., *Information Theory and Reliable Communication.* Wiley, New York, 1968.

4. Massey, J. L., "Coding and Modulation in Digital Communications," *Proc. International Zurich Seminar on Digital Communications,* 1974.

5. McEliece, R. J., *The Theory of Information and Coding.* Addison-Wesley, Reading, Mass, 1977.

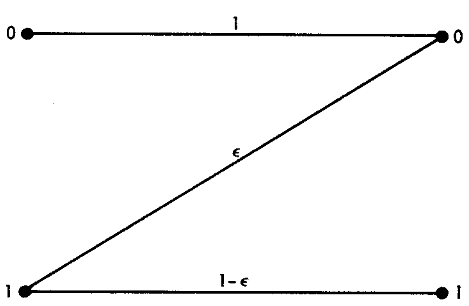

Fig. 1. The Z-channel

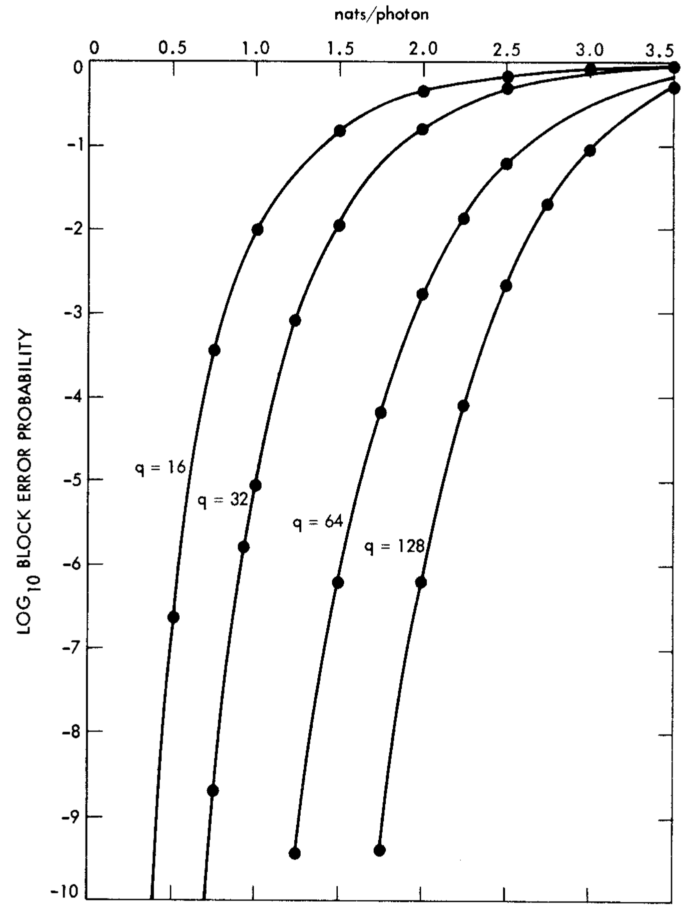

Fig. 2. Performance of some RS codes on the photon channel